View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Texas A&M Repository

International Journal of Communication 8 (2014), Feature 2603–2618 1932–8036/2014FEA0002


# "We Are Bradley Manning": Information Policy, the Legal Subject, and the WikiLeaks Complex

SANDRA BRAMAN
University of Wisconsin–Milwaukee, USA

In July 2013, WikiLeaks supporters took out a full-page advertisement in *The New York Times* with the banner headline "We Are Bradley Manning." The goal of all the signatories to the ad included in the "we" was to stand up for what they considered to be the important acts of citizenship in which they believed Manning to have engaged when he passed along diplomatic cables and other sensitive or classified material to the autonomous network.

The headline was more empirically accurate than signatories might have supposed. A profound challenge to the very concept of the nature of the legal subject is among the ways in which the suite of investigations and legal challenges of the WikiLeaks complex affect information policy and, in turn, law-state-society relations. U.S. government arguments used during Manning's seminal trial introduced a number of innovations in this area that could play critical roles going forward. Where these arguments are accepted, all those who signed the advertisement—indeed, all those who just followed news about WikiLeaks—might be considered liable.

Some of the information policy questions raised by the investigations and cases of the WikiLeaks complex are receiving a lot of attention, with online privacy and access to information about government activities notable among them. Others are less apparent, but it is not the extent of public awareness of an issue, the amount of media coverage devoted to it, or the amount of evidence available on one side or another that determines the relative importance of a given policy problem. Just as those involved in patent wars fight to own patents as early as possible in particular production processes as a means of controlling those processes in their entirety, so policy decisions, diversions, innovations, and reversals have their greatest impact when they challenge not only existing laws but policy-making processes themselves. Issues at stake in the WikiLeaks complex are of this kind.

By "information policy" we mean all laws, regulations, doctrinal principles, and practices affecting any kind of information creation, processing, flows, access, use, and destruction. More colloquially, information policy is an umbrella phrase referring to laws and regulations for information, communication, and culture. Information policy is particularly important among what political scientists call "issue areas," because it provides the context—the affordances and constraints—for all other decision making. Information policy is also the most reflexive aspect of a government, modulating the information flows within government and between a government and the rest of the world (Braman, 2007).

Copyright © 2014 (Sandra Braman, Sandra Braman: barman@uwm.edu). Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at http://ijoc.org.

This essay begins by thinking through just what we mean by the legal subject as an individual and collective identity. It goes on to look at the possible identities—and, therefore, legal subjects—intertwined in WikiLeaks as an exemplar of contemporary autonomous networks of political and legal importance. Where they are critical to the determination of a lawsuit, evidence of identities must be offered in court; the essay introduces some of the evidentiary questions upon which cases involving autonomous networks such as WikiLeaks will turn as introduced by the U.S. government during the Bradley Manning trial.

The information releases from cables and about the Iraq War were not the first, nor was information about governments the only type of information released. Matters involving national security, however, are unique among policy issue areas in their capacity to affect even the most fundamental doctrinal positions, matters at the constitutional level. With the cases arising out of Cablegate, there is also the first-mover advantage; the outcome of the Bradley Manning trial will in turn provide precedent (and evidence) that can then be used in other cases. Thus, it is upon the releases of cables and information about the Iraq War that this essay focuses.

Many governments are investigating matters raised by WikiLeaks and the many additional leaks from various sources that have taken place since Cablegate. References to U.S. law dominate here because of its relative importance in legal globalization processes, because it was the release of U.S. diplomatic cables that finally spurred governments around the world to engage with WikiLeaks, because the first trial of a person associated with WikiLeaks is taking place in the United States, and because of space and time limits. It would be valuable to learn how the same issues are working themselves out in the legal systems of other countries.

## The Legal Subject

In the face of the law, the question of personhood arises distinctly at at least three different levels: whether one is identifiable as a legal subject; whether one is subject to a specific legal jurisdiction (not the same thing as being a citizen); and whether one has standing, the right to be involved with a specific legal matter.[1] Here the focus is on the first of these.

Issues of personhood underlie many of today's most intense legal and political struggles. Participants in the Occupy, Indignado, and related social movements oppose corporate personhood altogether (apparently not realizing that if it were abolished, corporations could not be subjected to the law at all and the conditions about which those movements are concerned would only worsen). There are those for whom concern about "preborn children" justifies opposition to abortion (apparently not realizing that if the rights of generations to come must be taken into account legally, they become critical to environmental policy). Every possible variation on the theme has shown up in discussions about migration. The rights of the "nonhuman" have been receiving serious legal attention at least since the

[1] Standing relative to any given law or regulation begins with the requirement that the entity involved is subject to the legal system within which that law or regulation is embedded, but often goes beyond that to other characteristics or circumstances that are statute- or regulation-specific.

manuscript of Stone's (1975) memorable book, *Should Trees Have Standing?* was first sent to Supreme Court Justice William O. Douglas while the Court was considering a key environmental case. The extent and nature of legal rights, if any, of robots and intelligent software agents are being explored and are becoming increasingly salient. Governments are treated as legal individuals when they sue and are sued.

The right to recognition, or the right to legal personality, developed in the 17th century under the influence of the ideas of Hugo Grotius and Thomas Hobbes. Its initial uses were to create a means of conceptualizing various types of organizations as persons in order to subject them to the law. The Westphalian system of international relations, with its rules for diplomacy and war, worked because states were legal persons under international law. During the 19th century, corporations became full legal persons within national legal systems and during the 20th century, nongovernmental organizations did so as well. It was during the formation of the League of Nations in the early 20th century that the concept of the legal person began to be used in reference to individuals, considered the necessary first step for the protection of civil rights; the concern was to ensure that those groups often historically denied legal personhood—slaves, women, those who are stateless, children, and other marginalized groups—had rights as legal subjects. In a development pertinent to the struggles over issues raised by the WikiLeaks complex, President George W. Bush took the position that terrorist suspects were *not* legal persons under existing international law (Galchinsky, 2013).

WikiLeaks, as an autonomous network, takes us into this world because it is a type of collectivity that does not yet have formal status under the law. Figuring out just how to categorize various types of networks for legal purposes has become necessary given the growing influence of this mode of organizing. Legal systems classify social forms in order to implement—in social science terms, "operationalize"—the rules set down in laws and regulations that establish different rights and responsibilities for diverse entities. What we expect and require from a corporation is not the same as what we expect and require from a public interest advocacy group or a city government. Since categorizations affect how members of a group are perceived, there can be consequences for determinations of guilt and sentencing as well. In lawsuits involving WikiLeaks and other leaks of government information, the difference for a defendant between being perceived as a citizen whistleblower driven by a sense of political responsibility and being perceived as a terrorist treasonously attempting to destroy the country will be key.

With the WikiLeaks complex, there are not only many legal subjects but several concentric layers in an onion of ever-widening definitions of the subject. If the first type of legal subject involved in the complex of legal issues raised by WikiLeaks is the biological individual —Julian Assange, Bradley Manning, and others—the second is the WikiLeaks network. Just as characteristics of individuals affect how they are treated as legal subjects (Assange is an Australian citizen, Manning was in the U.S. military at the time of the alleged actions for which he has been charged), so characteristics of networks affect how they are treated by the law. A third type of legal subject is involved in the WikiLeaks complex as well, including the associational network of networks; for example, the intertwining of WikiLeaks and other autonomous networks such as Anonymous and Lulz could be used to justify treating the entirety as a single legal subject. And a fourth: If the legal subject of concern includes everyone who made use of the information from diplomatic cables released in Cablegate, it then includes, among many others, *The New York Times*, *The Washington Post*, and officials in the U.S. government. And a fifth: If the legal subject includes

everyone who read about WikiLeaks, the people involved, or the information released, the circle gets vastly larger. "We are," as the advertisement in *The New York Times* said, "Bradley Manning."

Thus, it becomes essentially impossible to imagine the individual who could not, according to some decision rule or another, be considered a legal subject with liability for WikiLeaks information releases. This is particularly the case where "lone wolf" rules apply (as in the United States), making loners who are not a part of social and communicative networks suspect for that reason alone. The WikiLeaks complex thus provides circumstances in which innovations conceptualizing the legal subject are being explored and the limits of the legal subject are being revisited.

## Who Is WikiLeaks?

Often we can, must, or will find it useful to distinguish WikiLeaks from Julian Assange. But there are times when the two are essentially equivalent, for Assange continues to drive the organization and serves as its public face. In a 2006 essay, "Conspiracy as Governance," Assange theorized about manipulating networks to undermine centers of power. Notably, he highlighted the strategic value of weak links, the marginal or relatively low-status individual; a defense in the Manning trial is that he would not (or should not) have had access to the information leaked at his low military rank. Assange concluded the essay by promising a next step, and shortly afterward launched WikiLeaks.

At the time of writing, Assange as an Australian citizen is under investigation for espionage by the U.S. government,[2] continues to fight extradition from house arrest in the United Kingdom to Sweden to respond to sexual charges, is or was the subject of a European campaign led by an Australian legislator to encourage the Swedish not to turn Assange over to the United States should he ultimately have to return to Sweden, and has taken on life as a media celebrity. Assange has launched an Australian political party that received under 1% of the votes in a recent election, the WikiLeaks organization became involved in the effort to protect subsequent leaker Edward Snowden (now living in Russia), and the Manning trial has concluded with a verdict of guilty on many charges but *not* of aiding and abetting the enemy, the treasonous charge that, upon conviction, can carry a death sentence. Still, there are others involved in WikiLeaks, there are individuals outside of WikiLeaks whose stories are essential to the shaping of legal responses to such information releases, and Assange as a person has a life that preceded and may succeed WikiLeaks.

The question of just how the legal subject is to be defined is not a matter only of concern to those who are themselves at the margins. Expanding the legal subject—from an individual, to a network, to a network of networks, to anyone using information, to anyone accessing information—is of profound importance. The advantages and disadvantages of such flexibility in definition of the legal subject have

2 In the United States, the charge under consideration at the time of writing would be espionage. Evidence brought to light in, and the ultimate determination of, the Bradley Manning trial will bear significantly on the extent to which the U.S. government believes it could have a case against Assange on this charge.

been demonstrated recently in uses of a concept of a particular type of legal subject—the terrorist—by governments around the world (Braman, 2011).

## Networks as Legal Subjects

It is easier to theorize, conceptualize, refer to, and even visualize networks than it is to understand them well enough for legal purposes. The counterterrorism effort, however, greatly stimulated interest in applying network theory when thinking about the legal subject (Borgen, 2008). It is not simply a matter of applying supposedly or allegedly neutral analytical techniques. Because models of networks effectively construct reality, "the integration of networks into legal descriptive contexts must be conducted very carefully. The unreflected adoption of their implied presumptions will inevitably clash with normative legal requirements" (Boysen et al., 2007, p. 1080). Where software agents trigger legal actions, problems raised by "posthuman law," in which machinic decision making replaces, supplants, or supersedes that of humans (Braman, 2002) pertain.

It was in the worlds of economics, technology, and the law that the practicalities of the transition to a network society first became sites of political struggles, conceptual innovation, legal creativity, programming expertise, and corporate experimentation. For economists, the network joins the market and the "hierarchy," or firm, as a third means of organizing economic transactions. The "network firm" is a corporation so entwined with others that the long-term project, rather than the firm or the industry, is the most valid unit of analysis; organizational boundaries are permeable and shifting; and cooperation and coordination are as important as competition for long-term economic success (Antonelli, 1992). Such economic networks leave traces in legal documentation such as contracts, agreements, financial reports, and filings; records of transactions, memberships, and client relationships; and other information, including e-mail and any documents circulated via e-mail that may become subject to legal scrutiny via the discovery processes that can precede trials. It is precisely the point that such traces are not available for autonomous networks that pride themselves on the anonymity and independent actions of their members and, in many cases, their rejection of the legitimacy of legal systems themselves.

This lack of formal legal traces can work both for and against a legal subject. It can provide protection, making it more difficult—though not impossible—for a government or Interpol to establish who members of groups such as WikiLeaks or Anonymous are. It can also, though, undermine or make impossible protections that might otherwise be available. The WikiLeaks failure to complete the website registration required to trigger coverage under the Swedish constitutional provision specifically protecting confidential sources of information (Jakobsson, 2011) means that the purported reason for locating WikiLeaks servers in that country would be irrelevant in a courtroom because the protections will not apply.[3]

3 Even where the same kinds of legal protections may exist in diverse legal cultures around the world, they may have very different origins. In the United States, there are protections for confidential sources of journalists, but these are based on interpretations of much more abstract constitutional language as developed across the guiding court decisions.

To technologists, a network is autonomous when it is decentralized, with content held on servers of member users rather than those of profit-oriented corporations. Xerox PARC will "soon" release technologies to support the formation of multiple privately controlled autonomous social networks for everyday use. The "unlike.us" electronic mailing list is one example of a group of individuals—in this case, those who work at the nexus of technology, art, and politics, who are trying to develop their own decentralized social networks. Legal anthropologists note that the growth of semiautonomous social fields interacts with the emergence of similarly semiautonomous legal systems (e.g., Shariff, 2008), the latter often described as "quasi-legal."

Autonomous networks such as WikiLeaks raise several problems for legal proceedings that include assigning accountability, determining who is within the network, and challenges to the nature of the legal processes themselves. Clarifying both concepts and practice vis-à-vis such networks is the current challenge.

## Individuals as Legal Subjects

Three ways in which the law interacts with individual identity are pertinent to the problem of anonymous networks as legal subjects: anonymity, professional identity, and citizenship. Online anonymity was under attack prior to Cablegate, but the effort to make it impossible has intensified. Professional identities provide filters on legal arguments. Citizenship involves not only jurisdictional and fealty issues but also positive obligations.[4]

### *Anonymity*

The importance of anonymous speech as a protection for those critical of government or of their employers has been legally recognized. Anonymity is often essential for whistleblowing (reporting on corporate or governmental misconduct that can harm individuals, groups, or society at large). In the commercial world, anonymity encourages some individuals to engage more freely in electronic commerce. Sociologically, anonymity makes it possible to experiment with personal identity online while participating in social media.

Anonymity can be chosen by oneself, accomplished statistically, or provided by another who protects the confidentiality of one's identity. The last of these in particular may bear on WikiLeaks cases. Courts acknowledge that legitimate reasons for protecting the confidentiality of a news source are myriad, reasonable, and strong. Individuals may be concerned about their safety and that of their families should it become known that they had spoken with journalists. Ongoing relationships with sources require mutual trust that could not be built without reliable promises of confidentiality. And there are certain subjects about which it is unlikely a journalist could ever acquire much information without having, in turn, assured

[4] For further discussion of the information policy implications of individual and collective identity—and relationships between the two—see the chapter, "Information Policy and Identity" and the accompanying bibliographic essay in Braman (2007).

the source of confidentiality. Protections of confidential news sources are legal acknowledgement of the importance of the news function to society.

In some familiar flavors, and some new, several factors place pressure on anonymity in the Internet environment. Arguments against permitting anonymity online include the needs to determine the legal jurisdiction under which an individual's activities fall, to surveil, and to implement mandated restrictions (such as age restrictions for pornography). The technological ability to track and retain detailed information about what individuals do online presents its own temptations. Protections have their limits in the competitive game of mathematics and computational capacity. Because that game can go through essentially infinite iterations, it should not be surprising that there are now full-blown commercial industries in both anonymizing technologies and the technologies used to break encryption and other anonymizing techniques.

The anonymizing setup of WikiLeaks was designed by Julian Assange, and owes a great deal to his programming prowess. It works so well, he claimed, that even he has no way of knowing whether Bradley Manning actually was the source of the Cablegate materials. One of the interesting features of the design is that it combines ancient techniques (just don't connect, here operationalized by creating an "air gap" between two computers with no links between them) with the very newest. Another is its inherent irony—Assange created a secrecy barrier around those who divulge the secrets of others.

### *Professional Identities*

Professionalism was an early-20th-century development that was part of the crystallization of distinctions among categories of knowledge and the bureaucratization of ever-more areas of life. Professionalism includes specialized training in accredited programs, licensing, continuing education, and a commitment to a profession-specific code of ethics. Medicine and the law are classical examples of professions in this sense. Used more loosely, the notion can be extended to any type of labor-based identity that filters relationships with particular laws and regulations, norms and expectations.

In information industries such as journalism and librarianship, professionalism has been sought and claimed. In many countries, though, professionalism has served more effectively as an ideal and a training tool rather than as a matter of formal bureaucratic recognition and practice. In the United States, for example, it is deemed unconstitutional to license journalists because of the opportunities licensing offers for control via regulation or threat of withdrawal of the license. Shy of formal professionalization, there are other jobs for which there are legal expectations regarding what can and cannot be said. Under securities regulation, for example, specific rules govern what information can be shared and under what conditions for those in diverse roles that range from financial advisor through those who provide tips. Labor law, too, has been an important source of job-related protections for and constraints upon speech of certain types. In the United States, it looks as if it will be labor law, for example, that provides the opening wedges for resistance to employer use of social network postings to terminate or otherwise punish employees.

Professional identities are important from a free speech perspective when protections for certain types of information exchanges are available only to those in particular professions. Relational privacy zones, for example, commonly protect most communications between individuals and doctors, lawyers, and religious confessors. The press has no special status under constitutional protections for free speech in the First Amendment in the United States, but a test has been developed that courts must meet to legitimately compel journalists to divulge their confidential sources of information or go to jail. About two-thirds of the states provide additional protection for the confidentiality of journalists' sources under "shield" laws.

The question of to whom this protection should apply has become problematic now that blogs, YouTube, Twitter, and other online media are being used for critically important journalistic purposes. Whether Assange should be considered a journalist is unclear. The extent to which WikiLeaks identified itself as a journalistic organization changed over time, moving toward a closer identification with the profession (Savage, 2010). During Cablegate, Assange crowed about having moved on to another level in the news organization hierarchy by serving as editor to the editors of news publications such as *The New York Times*, *The Guardian*, and *Der Spiegel* when they worked on details of the cable releases. That perception was not shared; then editor-in-chief of *The New York Times* Bill Keller (2011) described Assange's role as that of a source. Where journalists are professionals in the bureaucratic sense, with training and testing requirements, registration, and actual licensing, Assange will not qualify.

Bradley Manning's identity as a soldier who made pledges when he accepted his responsibilities significantly affects his case. His trial took place within the military rather than the civil justice system. Thus, although at the time it would have been unconstitutional to treat a U.S. citizen not in the military in this way, it was legal to imprison Manning indefinitely without charge. He was held under such tortuous conditions that it raised a public outcry and a government official resigned before Manning was moved to more tolerable conditions. A number of other elements of the trial procedure within the military justice system differ from those in the civil justice system.

### *Citizenship*

The identities of various players in the WikiLeaks complex as citizens of their respective countries have jurisdictional importance, filtering legal and political opportunities, contexts, and consequences. The number of countries that provide legal access to government information, for example, keeps growing, but significant differences exist across countries regarding just what that means; citizenship rights in this regard, then, vary by country. Differences across time periods within the same country also exist, including on the very interesting political and cultural question of just what it is that the good citizen needs to be informed about, as Schudson (1999) reminded us.

The WikiLeaks cases raise questions about who should have access to a particular government's information when that government's activities have global effect—questions already raised by those over the past couple of decades who have thought and acted in terms of global citizenship. A proposal for defining citizenship in terms of extent and relative likelihood of the effects of a given government on a particular individual already has been put forward (Koenig-Archibugi, 2012). Many significant WikiLeaks

releases have dealt with information from and about the private, not public, sector, provoking further social structures and processes. And there are questions about how citizens can meaningfully—not just noisily and with exuberance—express themselves in ways that can effectively influence political and legal decision making.

### *Collective Identity*

Additional identities accrue to individuals as a result of their participation in organizations, networks, and other collectivities—entities that are legal subjects as corporations, or nonprofit organizations, or neighborhood groups. Just as it is impossible to talk about the individual identity of the citizen without directly or indirectly, implicitly or explicitly, making assertions about the identity of the state (and vice versa), so it is impossible to talk about the identity of an autonomous network without making the same kinds of assertions about the individuals involved (and vice versa)—and about the nature of the associations themselves. Those who implement the law are among the many who now use network analysis tools and concepts. The specific features of autonomous networks, however, deserve specific attention as we think through the legal context for WikiLeaks.

## Network Analysis and the Law

The popularity of network analysis is in part a computational turn, for it was only in the 1990s that the software and computing capacity necessary to use such methods on large-scale networks became widely available. Not coincidentally, this was also when the Internet began to offer up a mass of networked flows of information begging for analysis using such tools. Additional growth in the use of these methods post-9/11 can be attributed to the combination of counterterrorism funds and political will as well as academic interest in theoretical and empirical developments.

Of course, there are many ways of studying networks that do not involve mathematically driven network quantitative analysis, any method has its weaknesses, and many important research questions exist for which network analysis is not helpful. Additional difficulties arise for using these methodological tools to study an autonomous network. When group borders are permeable, shifting, ambiguous, and anonymous by nature—as with WikiLeaks—which individuals should be considered members of a given network for legal purposes? What kinds of links among individuals are sufficiently pertinent to activities or intentions that they can validly be used as evidence? Are there any legal constraints on the means by which information to be used as evidence is collected? When there is neither a decision-making center nor any evident organizational hierarchy, where is legal culpability to be assigned? Who within a network should assume, in all senses of that word, liability? To what extent is a member of a network responsible for the activities of any other given individual within the same network, regardless of whether those activities were carried out in the network's name or whether those activities had been approved of and/or were known by that individual?

The first step in analysis of any contemporary information policy issue should be to contextualize it historically; a qualitatively new issue rarely appears. There is legacy law regarding associations among individuals both biological and fictive, claims of network autonomy, and confidentiality as a dialogic

relationship that bridges the individual and network levels of analysis at the link level. Beyond this terrain, most legal systems are just beginning to adapt to networks as legal subjects, although exploratory work in the legal and law and society literatures has been undertaken for several decades.

### *Legacy Law*

Several areas of legacy law feed into how we think about autonomous networks as legal subjects. Competition (antitrust) law focuses on the question of when informational relationships among the fictive individuals of corporations go beyond acceptable practice into legally unacceptable collusion. Discussion of constitutional protections for the right of association *per se* typically focuses on individuals who have left deliberate traces, in records, physical participation in group activities, and/or other visible signs of their membership in the group. And there is a history of providing the special privacy protections of confidentiality within the context of some types of professional relationships. Of the first two of these pertinent areas of legacy law, the history of the right of association is fairly well documented, but competition law is yet to be mined for what it offers regarding subtleties of informational relationships that might be of use in other legal domains.

Protection of the confidentiality of communications within professional relationships with physicians, attorneys, and religious confessors is particularly interesting for its theoretical provocations. With the importance of professionalism for some legal issues involving individual identity discussed above, this again highlights the rarely discussed importance of labor as a determinant of speech conditions. It is also significant that the types of relationships awarded confidentiality protections historically were "thick" in the Geertzian (1973) sense, comprised of many types of ties and rich in the amount of personal information shared, albeit often unidirectionally (from the layperson to the professional). The types of relationships asserted as meaningfully associative in WikiLeaks investigations fall at the other extreme of the spectrum of relative richness; they are as thin as possible, so thin we describe them as links rather than relationships, or even as interactions or transactions. Critiques of the replacement of thick knowledge of humans with the much thinner traces of bureaucratic records are replete. The links now being discussed as of interest for the purposes of determining legally important association are one or more orders of magnitude farther removed from the real humans involved than are such bureaucratic categories.

Gaps between thin information and thick humans raise two issues. The first involves warranting. Bureaucratic records require authority and authentication for there to be trust that a given set of records applies to the claimed individual; with links, the warranting claims themselves require warranting. The second involves limits to the kinds and extent of knowledge available based on thin informational records only; one may arrive at a website out of confusion, by mistake, for legitimate research purposes, because one was unwillingly diverted, or because of a technical failure. Arrival on a Web page does not mean that the page is read, far less what was made of it if so. The claim that having had access to a piece of information is in itself evidence of a meaningful relationship with other people—and of political intention and will—is an assertion that will often be invalid.

### *Autonomous Networks*

As a digital autonomous network, WikiLeaks has several characteristics that further confound efforts to clearly establish its identity as a legal subject. The group is inherently international and skews young. Involvement is not only anonymous but informal, voluntary, and may be ephemeral. Still, the network has scale, as demonstrated by the hundreds of mirror websites that appeared when Assange first went underground during Cablegate. Issues of network capacity, the value of weak links, and assumptions about indirect links by the security establishment, as briefly introduced in the next section, affect the nature of WikiLeaks as a legal subject.

Because many members of the network have significant programming skills, innovative digital tactics and strategies can be developed between and during campaigns. As is the case in any competition, changes in tactics and strategy make it more difficult for the opposing party to operate. Innovations can create phenomenological conditions different enough from those of other technologies that they require independent legal evaluation. In the long term, this feature of WikiLeaks and related contemporary practices stimulate the development of countertechnologies for use by those in the intelligence/security establishment. As such, they might be described as "pre-policy."

## Evidence

Where any of the individual, collective, or dialogic identities is asserted in the courtroom, evidence must be provided. The problem of how to reliably and validly determine the causal relations, intentions, and effects of various kinds of claimed informational relations is at the heart of the Bradley Manning trial. Some of the kinds of evidence and analysis presented will be familiar. Others may be less so, because they are generally obscure or because they are legal innovations. The incomplete list of possibilities that will receive attention includes material support, determining cause by effect, informational association, and indirect relationships.

### *Material Support*

The question of what it means to aid and support the enemy runs throughout the WikiLeaks complex. The answer matters, because it involves treason, the most serious of the possible charges available in situations involving leaks of government information. In the United States, treason is the only type of speech criminalized at the constitutional level, and those convicted of it can be put to death.[5]

The 18th-century constitutional language involving treason talks about providing "aid and comfort" to enemies and those with whom the United States is at war. Over time, the concept of comfort came to be interpreted as "providing material support." The 2001 USA PATRIOT Act defined material support to include training, expert advice or assistance, service, and personnel in provisions then applied to the provision of education in the peaceful use of legal means of seeking political change. Just a few

[5] The other 20 information policy principles in the U.S. Constitution offer positive principles upon which to base laws and regulations that affect speech and the speech environment (Braman, 2007).

months before Manning's pretrial hearing, the U.S. Supreme Court found this provision of the law constitutional in *Holder v. Humanitarian Law Project* (2011), a case in which the defendants were a group of lawyers involved in just such activities. As critics of the statute and of the decision argue, this expansion of the definition of treasonous speech to include training in how to peacefully and legally engage with political processes criminalizes peacekeeping efforts as well as those devoted to strengthening the rule of law.

The case involved an incident that took place before WikiLeaks was created, but the Supreme Court decision is important to cases involving the WikiLeaks complex. The fact that this was the one charge upon which Bradley Manning was ultimately *not* convicted sets important precedent for future cases that will evaluate the legitimacy of the sharing of politically important information, even though he was sentenced to 35 years in prison on other charges. Where the notion that material support can include education in the peaceful pursuit of legal means of political change, it will interact with treatment of indirect contacts (even where there are no intercedent links) as legally meaningful. In such a situation, association will be literally in the eyes of the beholder—the state. The state's imagination is likely to be stimulated by an interest in perceived associations of political import.

### *Determining Cause by Effect*

The novel argument that evidence of intention can be supplied by presenting documentation of effects appeared during Bradley Manning's pretrial hearing. The government argued that Zimbabwean government use of materials from the cables released by WikiLeaks is evidence that Manning intended to aid the enemy. This is particularly interesting, because there is also evidence that U.S. government officials made positive use of materials from the same cables, with some individuals making it known to the press that, from the government perspective, there had been positive uses of the released information.

Whatever picture of the overall effects of Cablegate is generated in the courtroom, to a social scientist, intentions and effects are two very different things. However good the evidence of one, it cannot tell you about the other. This is why, despite decades of effort to hold content producers liable when consumers of that content harm themselves or others by acting out that content in their own lives, it is difficult—if not impossible—to win such a case against the media. The idea of reversing the direction of the causality of social processes for legal purposes is not new with this evidentiary innovation, however. We saw it first in the USA PATRIOT Act's criminalization of activities that had taken place up to 15 years earlier—activities that were legal at the time they were undertaken.

### *Informational Association*

Though not historically referred to as such, legal interest in informational association has been around as long as banned books and forbidden languages. As is the case in many areas of the law affected by innovations in digital technologies, though, Engel's law—the rule that quantitative change can yield qualitative change—applies. In the online environment, the amount of information that can be accessed is orders of magnitude larger than would have been the case for anyone in the past, including those in centers of learning such as the Cambridges, English and American. That quantitative change in itself so

qualitatively changes the information environment that the notion of informational association not only deserves but requires reconsideration to develop foundational principles, legal arguments, laws and regulations, and implementation programs.

We also now have significantly greater capacity to analyze ever-increasing amounts of information in ever-more ways than was the case historically. What has been described by one scholar as a "mosaic" theory is being used to argue that the ability to combine, analyze, and make inferences from individual pieces of information can change legal access to information into illegal (Pozen, 2005). Recently, a version of this line of argument was used in defense of civil liberties in the U.S. Supreme Court decision in *US v. Jones* (2012), which held that it is unconstitutional for the government to use a GPS tracking device for extended periods without a search warrant because doing so crossed the line from the collection of individual pieces of information into a search. Such a theory, most likely under other rubrics, could appear in cases and investigations involving the WikiLeaks complex.

A genre argument is to be made as well. For its investigation of Assange, the U.S. government won a legal battle to gain access to information about individuals who were in communication with Assange and Manning via Twitter. To our knowledge from reports in the mass media, only a few key individuals identified as a result of this are now also subjects of investigation. However, the legal language in the government's request could be used to go after anyone who was tracking Twitter feeds about WikiLeaks and the information it released—even if only as a means of tracking the news.

There is a long history of special, effectively punitive, legal treatment of the news by governments desirous of silencing critical political debate. Stamp taxes, for example, including those which were among the immediate triggers to the American Revolution, add to the costs of producing and reading the news. It was during the presidency of George W. Bush that government officials first tried to discover the identity of an anonymous government critic by asking newspapers for information about who had read certain news stories cited in critiques. The U.S. government has now been told that it is constitutional to identify untold numbers of individuals around the world (given variable search terms and hashtags) as suspect targets simply because of an informational association that could be as thin as merely having received information about WikiLeaks via Twitter. Questions likely to be addressed if and when this position is challenged again include looking at whether the exposure to the information was witting or unwitting (that is, whether the person exposed to the information was aware of that exposure and cognizant of the information), whether the exposure was intended, whether the exposure was under normal or traumatic conditions (the biochemistry of memory works differently under traumatic conditions), whether the information was ever used, and whether any meaningful effects resulted from either the exposure to the information or its use.

Individuals in groups charged with terrorism have explicitly rejected the idea that people who share news about them were political associates and should be considered legally liable for actions being pursued. When members of a Turkish hacker group, RedHack, that had broken into government websites and leaked information were indicted with the possibility of facing up to 24 years in prison for being members of a terrorist group, RedHack argued: "Those 10 people have no ties with us; they are only

innocent people who shared the news [on online platforms] about us," a member of RedHack told a reporter (Güneş, 2012, para.3) in response to the indictment.

### *Indirect Contact*

Evidentiary issues discussed up to this point have included attention to genre, content, information uses, and network link formation via exposure to public third-party information. Some important conceptual developments regarding how to understand links themselves also have been made. The question of whether a link between Julian Assange and Bradley Manning was material enough to justify pursuing Assange was raised during the Manning pretrial hearing, and that type of question will repeatedly arise in cases involving members of autonomous networks. At some point what might potentially be called a link may be so attenuated, or the path so improbable, that it is not reasonable to treat it as a link at all. Early in 2011, the U.S. government announced that it had found no evidence of "direct contact" between Assange and Manning. By December, before Manning's pretrial hearing, the focus of the investigation was changed to "indirect contact." Evidence of this at a sufficient level to pursue Assange was presented during Manning's trial.

An interest in the political valence of extended associations was announced not long after 9/11, when then–Attorney General John Ashcroft suggested that those protecting homeland security should be exploring associations out to six degrees of separation. After leaving government in 2004, Ashcroft entered the world of business and, among other activities, joined the advisory board of a firm that has developed what it describes as innovative approaches to network analysis that start from the assumption that effective networks may be comprised of individuals among whom links are weak, indirect, or nonexistent, and thus not ordinarily visible. The company's software, the Lucid Threat Management System, identifies "previously unknown illicit networks that are hiding in plain sight" using existing information resources of a client to analyze network evolution and simulate and test interventions, manipulations, and constraints (Dulles Research, n.d., p. 1).

## The Question

The provocation for this essay was a 2011 invitation to think through how developments in the WikiLeaks complex affected the field of information policy. Important exemplars of informational issues affected by these developments include many that have received a significant amount of attention by others, such as its impact on the right to privacy and the appropriate limits of surveillance as well as free speech issues. Here attention has focused on challenges to the very nature of the legal subject in the network environment and new arguments that have been put forward by the U.S. government in the course of trying Bradley Manning—now Chelsea Manning—for leaking the material in what became known as Cablegate. Where those arguments are pushed to their limits, the network of concern for the actions for which he was convicted could, potentially, include any, and all, of us. And, thus, the legal insight as well as political rhetoric in the advertising heading, "We are Bradley Manning."

**References**

Antonelli, C. (1992). The economic theory of information networks. In C. Antonelli (Ed.), *The economics of information networks* (pp. 5–27). Amsterdam, The Netherlands: North-Holland.

Assange, J. (2006). Conspiracy as governance. Retrieved from me@iq.org (Julian Assange's old website, now obsolete).

Borgen, C. J. (2008). A tale of two networks: Terrorism, transnational law, and network theory. *Oklahoma City University Law Review*, *33*, 409–433.

Boysen, S., Buhring, F., Franzius, C., Herbst, T., Kotter, M., Kreutz, A., von Lewinski, K., et al. (2007). Networks in public law. *German Law Journal*, *8*, 1079–1089.

Braman, S. (2002). Posthuman law: Information policy and the machinic world, *First Monday*. Available at http://www.firstmonday.org/issues/issue7_12/braman/index.html

Braman, S. (2007). *Change of state: Information policy and power.* Cambridge, MA: MIT Press.

Braman, S. (2011). Anti-terrorism laws and the harmonization of media and communication policy. In R. Mansell & M. Raboy (Eds.), *Handbook of global media and communication policy* (pp. 486–504). Oxford, UK: Blackwell/Wiley.

Dulles Research. (n.d.) Home page. Retrieved from http://www.dullesresearch.com

Galchinsky, M. (2013). Quaint and obsolete: The "war on terror" and the right to legal personality. *International Studies Perspectives*, *14*, 255–268.

Geertz, C. (1973). Thick description: Toward an interpretive theory of culture. In C. Geertz, *The interpretation of cultures: Selected essays* (pp. 3–31). New York, NY: Basic Books.

Güneş, E. (2012, October 8). Hacker group faces up to 24 years in prison for "terrorist crimes." *Hürriyet Daily News*. Retrieved from http://www.hurriyetdailynews.com/hacker-group-faces-up-to-24-years-in-prison-for-terrorist-crimes.aspx?pageID=238&nID=31906&NewsCatID=339

*Holder v. Humanitarian Law Project*, 561 U.S. ___ (2010).

Jakobsson, P. (2011, July). WikiLeaks and Swedish law. Paper presented to the International Association of Media and Communication Research, Istanbul, Turkey.

Keller, B. (2011, January 26). Dealing with Julian Assange and the secrets he spilled. *The New York Times.* Retrieved from www.nytimes.com/2011/01/30/magazine/30Wikileaks-t.html

Koenig-Archibugi, M. (2012). Fuzzy citizenship in global society. *Journal of Political Philosophy*, *20*(4), 456–480.

Pozen, D. E. (2005). The mosaic theory, national security, and the Freedom of Information Act. *Yale Law Journal*, *115*, 628–679.

Savage, C. (2010, December 15). U.S. tries to build case for conspiracy by WikiLeaks. *The New York Times.* Retrieved from www.nytimes.com/2010/12/16/world/16wiki.html

Schudson, M. (1999). *The good citizen: A history of American civic life*. Cambridge, MA: Harvard University Press.

Shariff, F. (2008). Power relations and legal pluralism: An examination of "strategies of struggles" amongst the Santal Adivisi of India and Bangladesh. *Journal of Legal Pluralism, 57,* 1–43.

Stone, C. D. (1975). *Should trees have standing? Toward legal rights for natural objects*. New York, NY: Avon Books.

*U.S. v. Jones*, 565 US ___ (2012).